

- 28. Sozialversicherung
- 29. Krankenfürsorge
- 30. Gesundheitsversicherung
- 31. Verrechnungsservice
- 32. IKT-Gesundheitsservice

## Anlage 2: Zulässige Algorithmen

1. Alle Verfahren, die im Anhang der Signaturverordnung 2008 (SigV 2008), [BGBl. II Nr. 3/2008](#), in der jeweils geltenden Fassung, angeführt sind, sind zulässig.
2. Als symmetrische Verfahren sind geeignet:
  - AES (Advanced Encryption Standard) mit einer Schlüssellänge von 128, 192 oder 256 Bit [FIPS 197]
  - TDEA (Triple Data Encryption Algorithm) mit einer effektiven Schlüssellänge von mindestens 112 Bit [NIST 800-67]  
jeweils in CBC oder CTR Modus [NIST 800-38A].

Abkürzungen (zitierte Referenzen):

[FIPS 197]	„Advanced Encryption Standard (AES)“; National Institute of Standards and Technology (NIST); Federal Information Processing Standards Publication 197; November 2001.
[NIST 800-67]	„Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher“; National Institute of Standards and Technology; NIST Special Publication 800-67, Revision 1; 2012
[NIST 800-38A]	„Recommendation for Block Cipher Modes of Operation - Methods and Techniques“; National Institute of Standards and Technology; NIST Special Publication 800-38A; 2001.